

09 / 7 2 0 3 5 3

**VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT  
AUF DEM GEBIET DES PATENTWESENS**

**PCT**

**INTERNATIONALER RECHERCHENBERICHT**

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts <b>GR 99 P 6221 P</b>	<b>WEITERES VORGEHEN</b>	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5
Internationales Aktenzeichen <b>PCT/DE 00/ 01086</b>	Internationales Anmeldedatum (Tag/Monat/Jahr) <b>07/04/2000</b>	(Frühestes) Prioritätsdatum (Tag/Monat/Jahr) <b>30/04/1999</b>
Anmelder  <b>SIEMENS NIXDORF et al.</b>		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 2 Blätter.

☒ Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

**1. Grundlage des Berichts**

a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

☐ Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.

☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

☐ Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. ☐ **Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen** (siehe Feld I).

3. ☐ **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

**4. Hinsichtlich der Bezeichnung der Erfindung**

☒ wird der vom Anmelder eingereichte Wortlaut genehmigt.

☐ wurde der Wortlaut von der Behörde wie folgt festgesetzt:

**5. Hinsichtlich der Zusammenfassung**

☒ wird der vom Anmelder eingereichte Wortlaut genehmigt.

☐ wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 1

☒ wie vom Anmelder vorgeschlagen

☐ weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

☐ weil diese Abbildung die Erfindung besser kennzeichnet.

☐ keine der Abb.

# PATENT COOPERATION TREATY

**PCT**

## NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

Commissioner  
US Department of Commerce  
United States Patent and Trademark  
Office, PCT  
2011 South Clark Place Room  
CP2/5C24  
Arlington, VA 22202  
ETATS-UNIS D'AMERIQUE  
in its capacity as elected Office

Date of mailing: 09 November 2000 (09.11.00)	
International application No.: PCT/DE00/01086	Applicant's or agent's file reference: GR 99 P 6221 P
International filing date: 07 April 2000 (07.04.00)	Priority date: 30 April 1999 (30.04.99)
Applicant: NOLTE, Michael	

1. The designated Office is hereby notified of its election made:

☒ in the demand filed with the International preliminary Examining Authority on:  
25 August 2000 (25.08.00)

☐ in a notice effecting later election filed with the International Bureau on:

2. The election ☒ was

☐ was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

<p>The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland</p> <p>Facsimile No.: (41-22) 740.14.35</p>	<p>Authorized officer:</p> <p>J. Zahra</p> <p>Telephone No.: (41-22) 338.83.38</p>
--	--

## PATENT COOPERATION TREATY

09/720358

PCT

NOTICE INFORMING THE APPLICANT OF THE  
COMMUNICATION OF THE INTERNATIONAL  
APPLICATION TO THE DESIGNATED OFFICES

(PCT Rule 47.1(c), first sentence)

From the INTERNATIONAL BUREAU

To:

WINCOR NIXDORF GMBH & CO. KG  
Heinz-Nixdorf-Ring 1  
D-33106 Paderborn  
ALLEMAGNE

Date of mailing (day/month/year)

09 November 2000 (09.11.00)

Applicant's or agent's file reference

GR 99 P 6221 P

## IMPORTANT NOTICE

International application No.

PCT/DE00/01086

International filing date (day/month/year)

07 April 2000 (07.04.00)

Priority date (day/month/year)

30 April 1999 (30.04.99)

Applicant

WINCOR NIXDORF GMBH &amp; CO. KG et al

1. Notice is hereby given that the International Bureau has communicated, as provided in Article 20, the international application to the following designated Offices on the date indicated above as the date of mailing of this Notice:

US

In accordance with Rule 47.1(c), third sentence, those Offices will accept the present Notice as conclusive evidence that the communication of the international application has duly taken place on the date of mailing indicated above and no copy of the international application is required to be furnished by the applicant to the designated Office(s).

2. The following designated Offices have waived the requirement for such a communication at this time:

EP,NO

The communication will be made to those Offices only upon their request. Furthermore, those Offices do not require the applicant to furnish a copy of the international application (Rule 49.1(a-bis)).

3. Enclosed with this Notice is a copy of the international application as published by the International Bureau on 09 November 2000 (09.11.00) under No. WO 00/67422

## REMINDER REGARDING CHAPTER II (Article 31(2)(a) and Rule 54.2)

If the applicant wishes to postpone entry into the national phase until 30 months (or later in some Offices) from the priority date, a demand for international preliminary examination must be filed with the competent International Preliminary Examining Authority before the expiration of 19 months from the priority date.

It is the applicant's sole responsibility to monitor the 19-month time limit.

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

## REMINDER REGARDING ENTRY INTO THE NATIONAL PHASE (Article 22 or 39(1))

If the applicant wishes to proceed with the international application in the national phase, he must, within 20 months or 30 months, or later in some Offices, perform the acts referred to therein before each designated or elected Office.

For further important information on the time limits and acts to be performed for entering the national phase, see the Annex to Form PCT/IB/301 (Notification of Receipt of Record Copy) and Volume II of the PCT Applicant's Guide.

The International Bureau of WIPO  
34, chemin des Colombettes  
1211 Geneva 20, Switzerland

Facsimile No. (41-22) 740.14.35

Authorized officer

J. Zahra

Telephone No. (41-22) 338.83.38

Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

9/720353

Applicant's or agent's file reference GR 99 P 6221 P	<b>FOR FURTHER ACTION</b> See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/DE00/01086	International filing date (day/month/year) 07 April 2000 (07.04.00)	Priority date (day/month/year) 30 April 1999 (30.04.99)
International Patent Classification (IPC) or national classification and IPC H04L 9/32		
Applicant WINCOR NIXDORF GMBH & CO. KG		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 2 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☐ Certain observations on the international application

RECEIVED  
DEC 21 2001  
Technology Center 2100

Date of submission of the demand 25 August 2000 (25.08.00)	Date of completion of this report 02 May 2001 (02.05.2001)
Name and mailing address of the IPEA/EP	Authorized officer
Facsimile No.	Telephone No.

# INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/DE00/01086

## I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

- ☐ the international application as originally filed.
- ☒ the description, pages 1-8, as originally filed,  
 pages \_\_\_\_\_, filed with the demand,  
 pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_,  
 pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_.
- ☒ the claims, Nos. 9(in part), 10, as originally filed,  
 Nos. \_\_\_\_\_, as amended under Article 19,  
 Nos. \_\_\_\_\_, filed with the demand,  
 Nos. 1-8,9 (in part), filed with the letter of 28 February 2001 (28.02.2001),  
 Nos. \_\_\_\_\_, filed with the letter of \_\_\_\_\_.
- ☒ the drawings, sheets/fig 1/1, as originally filed,  
 sheets/fig \_\_\_\_\_, filed with the demand,  
 sheets/fig \_\_\_\_\_, filed with the letter of \_\_\_\_\_,  
 sheets/fig \_\_\_\_\_, filed with the letter of \_\_\_\_\_.

2. The amendments have resulted in the cancellation of:

- ☐ the description, pages \_\_\_\_\_
- ☐ the claims, Nos. \_\_\_\_\_
- ☐ the drawings, sheets/fig \_\_\_\_\_

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

# INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.  
PCT/DE 00/01086

## V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

### 1. Statement

Novelty (N)	Claims	1-10	YES
	Claims		NO
Inventive step (IS)	Claims	1-10	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-10	YES
	Claims		NO

### 2. Citations and explanations

CLAIMS 1, 9

The application pertains to a method and a device for signing messages and authenticating signatures thereof.

US-A-4 549 075 describes a method for preventing message falsification, a signature being formed with the assistance of symmetrical cryptography. Transmitters and receivers must have a common secret code that is stored securely.

WO-A-93/21711 describes a method for detecting the unauthorized reimportation or alteration of any data whatsoever transmitted by a transmitter to a receiver. The signature allocated to the useful data is symmetrically encoded using a combination of coupling data characterizing the coupling between the transmitter and the receiver and random data generated by a random generator. An alteration of the transmitted message can be detected in that the code used to encode the signature does not correspond to the code obtained by the receiver during decoding; accordingly, the decoded signature leads to an incorrect result.

In contrast, the control center and the receiver have a permanent and common master code, according to Claims 1 and 9. The control center pre-generates a sequence number from which a signature code is generated by means of a one-way function. The two are made available to the transmitter in a secure manner. By means of the signature code, the transmitter forms a signature for the message and transmits it with the sequence number and a message to the receiver. By means of the one-way function, master code, and sequence number, the receiver then forms a test code to test the signature of the message.

None of the available documents discloses such a method or device according to the features of Claims 1 and 9. Therefore, the subject matter of Claims 1 and 9 is regarded as novel and inventive (PCT Article 33(2) and (3)).

#### CLAIMS 2-8, 10

Dependent Claims 2-8 and 10 contain further details of said method according to Claim 1 and of the device as per Claim 9. Since they are dependent on Claims 1 and 9, they likewise meet the requirements pertaining to novelty and inventive step (PCT Article 33(2) and (3)).

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. .

PCT/DE 00/01086

**Supplemental Box**

(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: VII

Contrary to PCT Rule 5.1(a)(ii), the description does not cite search report citation WO-A-93/21711 or indicate the relevant prior art disclosed therein.



# VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

## PCT

REC'D 04 MAY 2001

### INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT



(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts GR 99 P 6221 P	WEITERES VORGEHEN siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsberichts (Formblatt PCT/IPEA/416)	
Internationales Aktenzeichen PCT/DE00/01086	Internationales Anmeldedatum (Tag/Monat/Jahr) 07/04/2000	Prioritätsdatum (Tag/Monat/Tag) 30/04/1999
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK H04L9/32		RECEIVED JUL 11 2001
Anmelder WINCOR NIXDORF GmbH & Co. KG et al.		Technology Center 2100

- Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationalen vorläufigen Prüfung beauftragten Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.
- Dieser BERICHT umfaßt insgesamt 5 Blätter einschließlich dieses Deckblatts.  
  
☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).  
  
 Diese Anlagen umfassen insgesamt 2 Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

- I ☒ Grundlage des Berichts
- II ☐ Priorität
- III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
- IV ☐ Mangelnde Einheitlichkeit der Erfindung
- V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
- VI ☐ Bestimmte angeführte Unterlagen
- VII ☒ Bestimmte Mängel der internationalen Anmeldung
- VIII ☐ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags  25/08/2000	Datum der Fertigstellung dieses Berichts  02.05.2001
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde:   Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Bevollmächtigter Bediensteter  Ferrari, J  Tel. Nr. +49 89 2399 8803 

# INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/DE00/01086

## I. Grundlage des Berichts

1. Hinsichtlich der **Bestandteile** der internationalen Anmeldung (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigefügt, weil sie keine Änderungen enthalten (Regeln 70.16 und 70.17)*):  
Beschreibung, Seiten:

1-8 ursprüngliche Fassung

RECEIVED

JUL 11 2001

**Patentansprüche, Nr.:**

Technology Center 2100

9 (Teil), 10 ursprüngliche Fassung

1-8, 9 (Teil) eingegangen am 28/02/2001 mit Schreiben vom 27/02/2001

**Zeichnungen, Blätter:**

1/1 ursprüngliche Fassung

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

Die Bestandteile standen der Behörde in der Sprache: zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um

- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).
- ☐ die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).
- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

- ☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.
- ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.
- ☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.
- ☐ Die Erklärung, daß die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

# INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/DE00/01086

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

- ☐ Beschreibung,      Seiten:
- ☐ Ansprüche,      Nr.:
- ☐ Zeichnungen,      Blatt:

RECEIVED

JUL 11 2001

Technology Center 2100

5. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

*(Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen; sie sind diesem Bericht beizufügen).*

6. Etwaige zusätzliche Bemerkungen:

## V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

### 1. Feststellung

Neuheit (N)	Ja: Ansprüche	1-10
	Nein: Ansprüche	
Erfinderische Tätigkeit (ET)	Ja: Ansprüche	1-10
	Nein: Ansprüche	
Gewerbliche Anwendbarkeit (GA)	Ja: Ansprüche	1-10
	Nein: Ansprüche	

2. Unterlagen und Erklärungen  
siehe Beiblatt

## VII. Bestimmte Mängel der internationalen Anmeldung

Es wurde festgestellt, daß die internationale Anmeldung nach Form oder Inhalt folgende Mängel aufweist:  
siehe Beiblatt

**Bemerkungen zum Absatz V.:**

**ANSPRÜCHE 1, 9**

Die Anmeldung betrifft ein Verfahren bzw. Einrichtung zur Signierung und Signaturprüfung von Nachrichten.

Dokument US-A-4 549 075 beschreibt ein Verfahren zur Fälschungssicherung von Nachrichten wobei mit Hilfe von symmetrischer Kryptographie eine Signatur gebildet wird. Absender und Empfänger müssen hierbei über einen gemeinsamen geheimen Schlüssel verfügen der sicher gespeichert sein muß.

Dokument WO 93/21711 beschreibt ein Verfahren zum Erkennen einer unberechtigten Wiedereinspielung bzw. Änderung beliebiger von einem Sender zu einem Empfänger übertragener Daten. Hierzu wird die den Nutzdaten zugeordnete Signatur symmetrisch unter Verwendung einer Kombination von die Kopplung zwischen Sender und Empfänger kennzeichnenden Kopplungsdaten und von einem Zufallsgenerator erzeugten Zufallsdaten verschlüsselt. Eine Änderung der übertragenen Nachricht kann dadurch erkannt werden, daß der zur Verschlüsselung der Signatur verwendete Schlüssel nicht dem bei der Entschlüsselung beim Empfänger gewonnenen Schlüssel entspricht und somit die entschlüsselte Signatur zu einem falschen Ergebnis führt.

Im Gegensatz hierzu, haben gemäß Anspruch 1, bzw. 9 die Zentrale und der Empfänger einen permanenten gemeinsamen Hauptschlüssel. Die Zentrale erzeugt vorab eine Sequenzzahl und aus dieser mittels einer Einwegfunktion einen Signierschlüssel. Beides wird gesichert dem Absender bereitgestellt. Der Absender bildet mittels des Signierschlüssels eine Signatur der Nachricht und sendet sie mit Sequenzzahl und Nachricht an den Empfänger. Der Empfänger bildet dann mittels Einwegfunktion, Hauptschlüssel und Sequenzzahl einen Prüfschlüssel und prüft damit die Signatur der Nachricht.

Keines der verfügbaren Dokumente offenbart ein solches Verfahren, bzw. Einrichtung, gemäß den Merkmalen des Anspruchs 1, bzw. 9. Neuheit sowie erfin-

derische Tätigkeit im Sinne des Artikels 33(2), (3) PCT des Gegenstands des Anspruchs 1 sowie 9 wird somit anerkannt.

#### **ANSPRÜCHE 2-8, 10**

Die abhängigen Ansprüche 2 bis 8 und 10 enthalten weitere Details des genannten Verfahrens gemäß Anspruch 1, bzw. der Einrichtung gemäß Anspruch 9. Da diese vom Anspruch 1 bzw. 9 abhängig sind, erfüllen sie ebenfalls die Erfordernisse gemäß Artikel 33 PCT bezüglich Neuheit und erfinderischer Tätigkeit.

#### **Bemerkungen zum Absatz VII.:**

Im Widerspruch zu den Erfordernissen der Regel 5.1 a) ii) PCT wird in der Beschreibung weder der in dem im Recherchenbericht zitierten Dokument WO 93/21711 offenbarte einschlägige Stand der Technik noch dieses Dokument selbst angegeben.

**Patentansprüche**

1. Verfahren zur Signierung einer Nachricht (22) durch einen Absender (20) und Prüfung der Signatur durch einen Empfänger, wobei eine Zentrale (10) und ein Empfänger (30) über einen geheimen gemeinsamen Hauptschlüssel (11, 11') verfügen, mit den Merkmalen:
- Die Zentrale (10)
    - \* erzeugt eine Sequenzzahl (12) und
    - \* aus dieser unter Verwendung des Hauptschlüssels (11) mittels einer Einweg-Verschlüsselung (13) einen Signierschlüssel (14) und
    - \* stellt dem Absender den Signierschlüssel (14) bereit;
  - der Absender (20)
    - \* bildet mittels des Signierschlüssels (14) eine Signatur (22c) über die Nachricht (21, 22c) und
    - \* sendet an den Empfänger einen Nachrichtensatz (22), der zumindest die Nachricht (22b) und die Signatur (22c), enthält.
  - Der Empfänger (30)
    - \* bestimmt die Sequenzzahl (22a'),
    - \* bildet ~~den~~ mittels der Einweg-Verschlüsselung (13') und dem Hauptschlüssel (11') einen Prüfschlüssel (14') und
    - \* prüft damit die Signatur (22c) der Nachricht.
2. Verfahren nach Anspruch 1, wobei die Sequenzzahl (12, 22a, 22a') zusammen mit dem Signierschlüssel (14) von

der Zentrale an den Absender (20) übergeben und von diesem über den Datensatz (22, 22') an den Empfänger übergeben wird.

3. Verfahren nach Anspruch 1, wobei die Sequenzzahl (12)  
5 durch einen Generator synchron zu der Anzahl der verwendeten Signier- bzw. Prüfschlüssel in der Zentrale (10) und bei dem Empfänger erzeugt wird.
4. Verfahren nach Anspruch 1, wobei die Sequenzzahl (12)  
10 durch einen Generator synchron zu der Anzahl der verwendeten Signier- bzw. Prüfschlüssel in der Zentrale (10) und bei dem Absender erzeugt und über den Datensatz (22, 22') an den Empfänger übergeben wird.
5. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Sequenzzahl durch einen Generator für Pseudo-  
15 Zufallszahlen erzeugt wird.
6. Verfahren nach einem der vorhergehenden Ansprüche, wobei als Einweg-Verschlüsselung die Verschlüsselung der Sequenzzahl mittels des Hauptschlüssels verwendet wird.
7. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Zentrale (10) vorab mehrere Signierschlüssel  
20 (14) erzeugt und diese, ggf. sofern zweckmäßig, gemeinsam mit den zugehörigen Sequenzzahlen (12), an den Absender (30) übermittelt.
8. Verfahren nach einem der vorhergehenden Ansprüche, wobei der Empfänger (30) eine Liste bereits verwendeter  
25 Sequenzzahlen führt und bereits verwendete Sequenzzahlen abweist.
9. Einrichtung zur Signierung einer Nachricht (22, 22'), die von einem Absender (20) an einen Empfänger (30) geschickt wird, mit den Merkmalen:  
30